NORTH CAROLINA BANKING INSTITUTE

Volume 21 | Issue 1 Article 15

3-1-2017

First Time for Everything: The CFPB Enforces Data Security

Graham T. Dean

First Time for Everything: The CFPB Enforces Data Security

I. INTRODUCTION AND BACKGROUND

In March 2016, the Consumer Financial Protection Bureau ("CFPB") filed its first data security enforcement action against Iowa-based fintech firm, Dwolla, Inc. ("Dwolla").[1] The consent order resulting from this action details how Dwolla's data security statements were deceptive, and orders Dwolla to implement a host of new measures aimed at better protecting its customers' personal information.[2] This action raises many new questions surrounding the CFPB's role in policing data security, and how this agency's actions will compare to those pursued by other regulators, including the similarly situated Federal Trade Commission ("FTC").[3] In the absence of further actions and guidance, "covered persons"[4] should look to the recommendations outlined in the Dwolla consent order, because, as of now, it remains the most useful source for predicting how the CFPB will regulate data security in the future.[5]

Financial institutions often possess vast amounts of consumer information, the value of which places them amongst the most popular targets for cyber attack.[6] On the black market credit card numbers can

1. Dwolla, Inc. CFPB No. 2016-CFPB-0007 *1 (Mar. 2, 2016) [hereinafter Dwolla Consent Order].

2. *Id.*

3. *See* WILL DURBIN & YENISEY RODRIGUEZ, PAUL WEISS, RIFKIND, WHARTON & GARRISON LLP, THE CFPB ENTERS THE CYBERSECURITY ARENA WITH ITS FIRST ENFORCEMENT ACTION 4 (2016), https://www.paulweiss.com/media/3377203/4mar16cyberalert.pdf.

4. Dodd-Frank Wall Street Reform and Consumer Protection Act ("Dodd-Frank") § 1002, 12 U.S.C. § 5481(6) (2015) ("The term 'covered person' means—(A) any person that engages in offering or providing a consumer financial product or service; and (B) any affiliate of a person described in subparagraph (A) if such affiliate acts as a service provider to such person.").

5. *See* Durbin & Rodriguez, *supra* note 3, at 4 ("Among other sources, companies should look to the remedial actions that the CFPB required of Dwolla for guidance on how to strengthen their systems.").

6. IBM, 2016 COST OF DATA BREACH STUDY 7 (2016), https://public.dhe.ibm.com/common/ssi/ecm/se/en/sel03094usen/SEL03094USEN.PDF.

sell for $15 each, while more comprehensive "Fullz"[7] information packages can sell for twice that.[8] As a result of storing such valuable information, companies in the financial sector experience above average remediation costs when data breaches do occur.[9] Industry observers note that the occurrence rate of data breaches is increasing, with 554 million consumer records compromised in the first half of 2016 alone.[10] Over the course of the last decade, the average cost of corporate data breaches has also increased, from $3.5 million in 2006 to an estimated $7 million in 2016.[11] Nearly 15% of this cost is associated with legal defense services, while a loss of customer confidence accounts for about 40% of the cost.[12]

Preventing these attacks can be difficult, as cybercriminals are constantly adapting their methods of attack.[13] While the recent shift to EMV[14] credit card chip technology has improved the security of card-present transactions, this change has also had the unanticipated effect of increasing the amount of digital financial fraud.[15] Experts predict that cybercriminals will begin to shift focus to the financial sector's growing number of non-traditional institutions, such as mobile payment systems

7. "Fullz" includes "identity information, which can include full name, email address and password, physical address, phone number, date of birth, Social Security Number, driver's license number, bank name, bank account number, bank routing number, victim employer's name." LILLIAN ABLON ET AL., RAND CORP., MARKETS FOR CYBERCRIME TOOLS AND STOLEN DATA 49 (2014), http://www.rand.org/content/dam/rand/pubs/research_reports/RR600/RR610/RAND_RR610.pdf.

8. CHARLES MCFARLAND ET AL., MCAFEE, THE HIDDEN DATA ECONOMY 5 (2015), http://www.mcafee.com/us/resources/reports/rp-hidden-data-economy.pdf?clickid=RsiVUn3BAVPg1wUwJ52—UvmUkkTQ5zExAN380&lqmcat=Affiliate:IR:null:74047:10078:10078:null&sharedid=.

9. *See* IBM, *supra* note 6, at 7 (illustrating that the financial industry has an above average per capita breach cost)

10. *Gemalto Releases Findings of First Half 2016 Breach Level Index*, GEMALTO (September 20, 2016) http://www.gemalto.com/press/Pages/Gemalto-releases-findings-of-first-half-2016-Breach-Level-Index.aspx.

11. IBM, *supra* note 6, at 6.

12. IBM, *supra* note 6, at 16.

13. *See* Penny Crossman, *Are You Ready for the Cybersecurity Challenges of 2016?*, AM. BANKER (Jan. 5, 2016), https://www.americanbanker.com/news/are-you-ready-for-the-cybersecurity-challenges-of-2016 (writing how new technologies can spur new methods of cyberattack).

14. EMV stands for Europay, MasterCard and Visa, which have collectively developed the new standard credit cards, which utilize harder-to-counterfeit chips rather than traditional magnetic strips. Oren Levy, *Europay, MasterCard, Visa: A Primer*, TECHCRUCH (May 12, 2015), https://techcrunch.com/2015/05/12/europay-mastercard-visa-a-primer/.

15. Crossman, *supra* note 13.

and transfer products.[16]

The CFPB was established in 2011 as part of the Dodd–Frank Wall Street Reform and Consumer Protection Act ("Dodd-Frank").[17] The purpose of the CFPB is to enforce federal consumer financial laws on behalf of consumers, and to ensure that markets for consumer financial products and services are "fair, transparent, and competitive."[18] Interpreting this delegation of power broadly, the CFPB regulates traditional financial institutions in addition to a diverse range of groups traditionally conceptualized as being non-financial (i.e. merchants, retailers, and real estate agents.)[19] The CFPB also has authority to police a variety of "enumerated consumer laws," including the Electronic Fund Transfer Act, the Truth in Savings Act, and the Consumer Leasing Act.[20] In addition, the CFPB has the primary authority to enforce federal consumer financial laws over depository institutions with assets greater than $10 billion.[21]

This Note analyzes the implications of the *Dwolla* enforcement action, and proceeds in four parts. Part II examines the findings and recommendations made by the CFPB in the *Dwolla* Consent Order.[22] Part III outlines how other federal and state regulators have policed data security, with a focus on the FTC's enforcement.[23] Finally, Parts IV and V discuss the practical implications of *Dwolla* and the steps that financial institutions should take to avoid similar enforcement actions.[24]

16. Crossman, *supra* note 13.

17. *See* Dodd-Frank Wall Street Reform and Consumer Protection Act ("Dodd-Frank") § 1021, 12 U.S.C. § 5511 (2015) (establishing the purpose, objectives, and function of the CFPB).

18. Dodd-Frank § 1021, 12 U.S.C. § 5511 (2015); CONSUMER FIN. PROT. BUREAU, CFPB SUPERVISION AND EXAMINATION MANUAL (Oct. 2012) http://files.consumerfinance.gov/f/201210_cfpb_supervision-and-examination-manual-v2.pdf.

19. Dodd-Frank § 1024, 12 USC § 5514 (2015); MORGAN, LEWIS & BOCKIUS LLP, THE CONSUMER FINANCIAL PROTECTION BUREAU: WHAT IT IS AND WHAT TO EXPECT (Jan. 2012), https://www.morganlewis.com/pubs/lit_whitepaper_consumerfinancialprotectionbureau_jan2012.pdf at 5.

20. ARNOLD & PORTER LLP, THE DODD-FRANK ACT ESTABLISHES THE CONSUMER FINANCIAL PROTECTION BUREAU AS THE PRIMARY REGULATOR OF CONSUMER FINANCIAL PRODUCTS AND SERVICES 2 (July 2010), http://files.arnoldporter.com/advisory—the_dodd-frank_act_establishes_the_consumer_financial_protection_bureau_071510.pdf.

21. *Id.* at 6.

22. *See infra* Part II.

23. *See infra* Part III.

24. *See infra* Part IV & V.

II. DWOLLA GOES FIRST

Founded in 2010, Dwolla offers digital money transferring services similar to those provided by PayPal and Venmo.[25] Dwolla users can transfer money both to and from accounts managed entirely online, accessible through a variety of digital platforms.[26] The money stored in a Dwolla account can be transferred directly to the consumer's bank account or stored indefinitely in the user's Dwolla-managed account.[27] The money stored in Dwolla-managed accounts is held in bank accounts managed by Compass Bank and Veridian Credit Union.[28] When users register for an account, they are asked to provide their name, address, date of birth, and Social Security number.[29] This information is stored by Dwolla both for communication purposes and for use in subsequent transactions.[30] Customers are asked to provide a routing number and an account number if they elect to link a separate bank account.[31] At the time of this enforcement action, Dwolla had approximately 653,000 users and was transferring approximately $5 million a day.[32]

The main assertion of the CFPB's enforcement action is that Dwolla engaged in "deceptive acts and practices relating to false representation regarding respondent's data security practices in violation of Sections 1031(a) and 1036(a)(1) of the Consumer Financial Protection Act of 2010."[33]

After establishing jurisdiction and definitions, the consent order summarizes the findings of the CFPB's investigation of Dwolla's data security policy.[34] The deceptive acts at issue in this matter took place from January 2011 to March 2014.[35] Seven deceptive representations

25. *Our Story*, DWOLLA, INC., https://www.dwolla.com/press (last visited Jan. 24, 2017).

26. *Id.*

27. *Id.*

28. DWOLLA CONSENT ORDER, *supra* note 1, at *4.

29. DWOLLA CONSENT ORDER, *supra* note 1, at *4.

30. *See* DWOLLA CONSENT ORDER, *supra* note 1, at *4 (establishing what contact information Dwolla user's must provide during registration).

31. DWOLLA CONSENT ORDER, *supra* note 1, at *4.

32. DWOLLA CONSENT ORDER, *supra* note 1, at *5.

33. DWOLLA CONSENT ORDER, *supra* note 1, at *1.

34. DWOLLA CONSENT ORDER, *supra* note 1, at *1–10 ("The Bureau has jurisdiction over this matter under Sections 1053 and 1055 of the CFPA, 12 U.S.C. §§ 5563 and 5565.").

35. DWOLLA CONSENT ORDER, *supra* note 1, at *5.

are listed, all of which were claims made by Dwolla on its website.[36] These representations included claims that customer data was "securely encrypted and stored," and that Dwolla utilized "the latest encryption and secure connections" technologies.[37] Elsewhere, Dwolla claimed its security practices "exceed[ed] industry standards" and set "a new precedent for the industry for safety and security."[38]

The consent order also details a simulated attack previously conducted by Dwolla during which 62% of its employees clicked on a vulnerable link, and 25% of its employees gave up access to customer information.[39] Despite these results, Dwolla failed to train employees or take any other affirmative steps to prevent such attacks.[40] The CFPB does not allege that an actual data breach took place, nor does it allege anyone ever attempted to retrieve consumer data from Dwolla's servers.[41]

The CFPB issued Dwolla a $100,000 penalty, which is an extraordinarily low figure compared to monetary penalties issued by the CFPB in the past.[42] All of the penalties resulting from this action went into the CFPB's general Civil Penalty Fund, which is used to compensate victims in other enforcement actions brought by the agency.[43] To put this figure in perspective, in 2014 over 40% of the CFPB's actions resulted in penalties in excess of $5 million, with two exceeding $10 million.[44] One of the CFPB's largest settlements came in 2007 when Bank of America agreed to pay $727 million for a variety of violations, including deceptive marketing of its credit card products.[45]

36. DWOLLA CONSENT ORDER, *supra* note 1, at *6.

37. DWOLLA CONSENT ORDER, *supra* note 1, at *6.

38. DWOLLA CONSENT ORDER, *supra* note 1, at *5.

39. DWOLLA CONSENT ORDER, *supra* note 1, at *8.

40. DWOLLA CONSENT ORDER, *supra* note 1, at *8.

41. *See* DWOLLA CONSENT ORDER, *supra* note 1, at *8 (failing to mention any breaches or attempts to breach Dwolla's servers).

42. DWOLLA CONSENT ORDER, *supra* note 1, at *16.

43. DWOLLA CONSENT ORDER, *supra* note 1, at *16; CONSUMER FIN. PROT. BUREAU, *Civil Penalty Fund*, http://www.consumerfinance.gov/about-us/payments-harmed-consumers/civil-penalty-fund/.

44. JOSEPH L. BARLOON, ANAND S. RAMAN & AUSTIN K. BROWN, SKADDEN, ARPS, SLATE, MEAGHER & FLOM LLP, CFPB DEFINES 'UNFAIR,' 'DECEPTIVE' AND 'ABUSIVE' PRACTICES THROUGH ENFORCEMENT ACTIVITY (Jan. 2015), https://www.skadden.com/insights/cfpb-defines-unfair-deceptive-and-abusive-practices-through-enforcement-activity.

45. *CFPB Orders Bank of America to Pay $727 Million in Consumer Relief for Illegal Credit Card Practices*, CONSUMER FIN. PROT. BUREAU (Apr. 9, 2014),

Alternatively, the relatively small penalty issued to Dwolla could be due to the unprecedented nature of this action.[46] Furthermore, the small penalty potentially could have been strategic, in that it may have discouraged Dwolla from litigating the validity of this unprecedented action.[47]

For Dwolla, implementing the changes mandated in the consent order will likely exceed the cost of the monetary fine.[48] The order somewhat broadly instructs Dwolla to "adopt and implement reasonable and appropriate data security measures to protect consumers' personal information."[49] The CFPB further requires that Dwolla "improve the safety and security of its operations and the consumer information that is stored on, or transmitted through its networks."[50] To accomplish these improvements the consent order provides some specific steps that Dwolla must take, including the establishment of a data security plan and the hiring of "a qualified person" to coordinate and account for Dwolla's data security.[51] The consent order also requires Dwolla to conduct two annual network security assessments, after which any identified issues are remedied.[52]

The order further provides that Dwolla must report certain information to the CFPB for a period of at least five years.[53] These reports must include a list of employees handling data security issues as well as any training materials, risk assessments, or advertisements relating to data security.[54] While five years of reporting may seem excessive, it pales in comparison to data security actions brought by other agencies, some of which consist of decades of direct supervision.[55]

---

http://www.consumerfinance.gov/about-us/newsroom/cfpb-orders-bank-of-america-to-pay-727-million-in-consumer-relief-for-illegal-credit-card-practices/.

46. *See* DURBIN & RODRIGUEZ, *supra* note 3 (stressing the fact that this is the first data security related action brought by the CFPB).

47. *See* DURBIN & RODRIGUEZ, *supra* note 3

48. *See* DURBIN & RODRIGUEZ, *supra* note 3 (listing the multiple steps that have to be taken by Dwolla to comply with the consent order).

49. DWOLLA CONSENT ORDER, *supra* note 1, at *11.

50. DWOLLA CONSENT ORDER, *supra* note 1, at *11.

51. DWOLLA CONSENT ORDER, *supra* note 1, at *12.

52. DWOLLA CONSENT ORDER, *supra* note 1, at *12.

53. DWOLLA CONSENT ORDER, *supra* note 1, at *19.

54. DWOLLA CONSENT ORDER, *supra* note 1, at *19–20.

55. *See Fandango, Credit Karma Settle FTC Charges That They Deceived Consumers by Failing to Securely Transmit Sensitive Personal Information*, FED. TRADE COMM'N, (Mar. 28, 2014), https://www.ftc.gov/news-events/press-releases/2014/03/fandango-credit-

In the short term, the order instructs Dwolla to submit a compliance report within 90 days,[56] and conduct a data security audit within 180 days.[57] During the audit, Dwolla must allow a "qualified person" to evaluate the effectiveness of the policies being implemented, who will then report whether Dwolla is complying with the consent order.[58] In the event that the requirements of this consent order are not met, there are procedures by which the CFPB can extend the duration of its supervision.[59]

III. REGULATING IN A CROWDED FIELD

The legal landscape governing data security is crowded, with forty-seven laws relating to data breach notification alone.[60] Relevant to financial institutions, the Federal Deposit Insurance Corporation ("FDIC"), Federal Reserve Board ("FRB"), and Office of the Comptroller of the Currency ("OCC") all regulate data security in some capacity.[61] Collectively, these agencies have acted on data security in their roles as members of the Federal Financial Institutions Examination Council ("FFIEC").[62] These agencies have also issued independent data security guidance and regulations, the focus of which varies based on their respective powers and jurisdiction.[63]

karma-settle-ftc-charges-they-deceived-consumers.

56. DWOLLA CONSENT ORDER, *supra* note 1, at *14, 18.

57. DWOLLA CONSENT ORDER, *supra* note 1, at *12.

58. DWOLLA CONSENT ORDER, *supra* note 1, at *14.

59. DWOLLA CONSENT ORDER, *supra* note 1, at *15-16.

60. Judith Germano, *Proposed New York Cybersecurity Regulation: A Giant Leap Backward?*, FORBES (Dec. 2, 2016, 2:32 PM), http://www.forbes.com/sites/realspin/2016/12/02/proposed-ny-cybersecurity-regulation-a-giant-leap-backward/#61367f462e78.

61. *See, e.g.*, Press Release, Bd. of Governors of the Fed. Reserve Sys., Agencies Issue Advanced Notice of Proposed Rulemaking on Enhanced Cyber Risk Management Standards (Oct.19, 2016), https://www.federalreserve.gov/newsevents/press/bcreg/20161019a.htm (discussing a recent proposed rule set forth by these agencies).

62. DEBOVOISE & PLIMPTON LLP, CLIENT UPDATE: FEDERAL FINANCIAL REGULATORS TO PROPOSE ENHANCED CYBER RISK MANAGEMENT STANDARDS (Oct. 25, 2016), http://www.debevoise.com/~/media/files/insights/publications/2016/10/20161025_federal_financial_regulators_to_propose_enhanced_cyber_risk_management_standards.pdf.

63. *See, e.g.*, JEFFREY SACKS, CROWE HORWATH LLP, FDIC INTREX PROGRAM IS HERE (Sept. 6 2016), http://www.crowehorwath.com/cybersecurity-watch/fdic-intrex-program/?utm_source=feedburner&utm_medium=email&utm_campaign=Feed%3A+CroweCybersecurityWatch+%28Crowe+Cybersecurity+Watch%29 (discussing a program instituted by the FDIC, applying narrowly to insitutions covered by that agency).

Notably, the FFIEC recently issued data security guidance requiring large financial institutions[64] to implement "enhanced standards" for data security.[65] This guidance recognizes current regulations,[66] and mandates that certain large institutions go even further.[67] Many of the requirements in this guidance are specific and technical in nature. One such requirement is that companies establish a two-hour Recovery Time Objective ("RTO"), during which they recover all compromised data and restore systems in the event of a data breach.[68] In 2005, the FFIEC published *The Interagency Final Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice*.[69] Scholars have criticized this publication as only providing limited practical steps, and failing to lay out the definitive guidance the industry needs.[70]

Some of the most notable regulations at the federal level have come in response to the Financial Services Modernization Act of 1999, known more commonly as the Gramm-Leach-Bliley Act ("GLBA").[71] Title V of the GLBA addresses the potential dangers that financial mergers create for non-public consumer information, and requires that federal agencies establish administrative, technical, and physical

64. Applying to holding companies with total assets exceeding $50 billion, companies that manage financial market infrastructure, and nonbank financial companies covered by the Federal Reserve Board. Including the FFIEC Cybersecurity Assessment Tool and the NIST Cybersecurity Framework. FED. RESERVE SYS., ENHANCED CYBER RISK MANAGEMENT STANDARDS 11 (Oct.19, 2016), https://www.federalreserve.gov/newsevents/press/bcreg/bcreg20161019a1.pdf.

65. *Id.* at 1.

66. *Id.*

67. *Id.* at 11 ("Similar to the NIST CSF, the enhanced standards would provide a clear set of objectives for sound cyber risk management. However, the binding requirements set forth in the enhanced standards would be designed specifically to address the cyber risks of the largest, most interconnected U.S. financial entities.").

68. *Id.* at 41.

69. Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice, 70 Fed. Reg. 15736 (Mar. 29, 2005) (to be codified at 12 C.F.R. pts. 30, 208, 225, 364, 568, and 570).

70. *See* ALEJANDRO H. CRUZ & CRAIG A. NEWMAN, PATTERSON BELKNAP WEBB & TYLER LLP, OCC'S CYBERSECURITY REGULATORY EXPECTATIONS (Jan. 7, 2016), https://datasecuritylaw.com/occs-cybersecurity-regulatory-expectations-a-call-to-action/ (explaining how past OCC guidance was primarily found in documents published collectively in their capacity as members of the FFIEC).

71. Financial Services Modernization Act ("Gramm-Leach-Bliley Act") § 1093(1), 15 U.S.C. § 6801 (2015). *The Gramm-Leach-Bliley Act*, ELEC. PRIVACY INFO. CTR., https://epic.org/privacy/glba/ (last visited Jan. 24, 2017).

controls for protecting this information.[72] Specifically, the GLBA requires federal agencies to implement safeguards for financial institutions that ensure the security of customer information, protect against anticipated threats, and prevent unauthorized access that could result in substantial harm or inconvenience to customers.[73] GLBA was amended in 2010 to explicitly exclude the CFPB from the list of agencies required to implement the law.[74]

The FDIC issued its own data security recommendations in 1996, three years prior to the passing of the GLBA.[75] The jurisdiction of the FDIC is broad, extending over all banks and saving associations that participate in the FDIC insurance program.[76] This agency's guidance has often concerned specific technical issues relevant at the time, addressing issues as narrow as the dangers of employee instant messaging at banks.[77] To monitor cybersecurity, the FDIC utilizes regulatory and intelligence reports in addition to identifying issues at specific banks through the FDIC examination process.[78] The FDIC may use enforcement actions against institutions that fail to remedy issues identified during these examinations.[79] In 2015, the FDIC implemented a new Information Technology Risk Examination ("InTREx") program that updates previous examination techniques by placing an increased focus on data security, particularly in regard to emerging technologies such as mobile banking.[80] With approximately two decades of FDIC guidance on security, many institutions insured by the FDIC already

72. Gramm-Leach Bliley Act § 1093(1), 15 U.S.C. § 6801.

73. *Id.* at § 6801(b).

74. *Id.*

75. *Cybersecurity and Information Security: FDIC Financial Institution Letters*, FED. DEPOSIT INS. CORP., https://www.fdic.gov/regulations/resources/director/risk/it-security.html (last visited Jan. 24, 2017).

76. Federal Deposit Insurance Act § 2, 12 U.S.C. § 1814(a)(2015).

77. *See Regulatory Guidance: Cybersecurity and Information Security: FDIC Financial Institution Letters*, FED. DEPOSIT INS. CORP., https://www.fdic.gov/regulations/resources/director/risk/it-security.html (listing the specific titles of past FDIC letters relating to data security) (last visited Jan. 24, 2017).

78. *A Framework for Cybersecurity*, 12 SUPERVISORY INSIGHTS 7, FED. DEPOSIT INS. CORP. (Dec. 2015), https://www.fdic.gov/regulations/examinations/supervisory/insights/siwin15/SI_Winter2015.pdf.

79. FED. DEPOSIT INS. CORP., FDIC COMPLIANCE EXAMINATION MANUAL II-1.1 (Dec. 2015) https://www.fdic.gov/regulations/compliance/manual/2/II-1.1.pdf.

80. Sacks, *supra* note 63.

have sophisticated data security policies in place.[81]

While certainly less involved than the FDIC, the FRB has also regulated data security with a strong consumer-based approach.[82] The FRB's guidance began in response to the requirements found the GLBA.[83] These original provisions made no mention of digital threats, but more generally instructed covered entities to have written information protection plans in place that included physical safeguards "appropriate to the size and complexity of the bank and the nature of its activities."[84] Beyond this initial guidance, the vast majority of the guidance issued by the Federal Reserve has been published in cooperation with its FFIEC counterparts.[85]

Finally, the OCC has been somewhat active in ensuring data security for the national banks and federal savings associations under its jurisdiction.[86] The OCC unilaterally issues semi-annual risk assessments for federally chartered institutions, which in recent years have highlighted data security as a primary concern.[87] The most recent OCC risk assessment notes that the threat of cyber attack is increasing as banks continue to adopt new digital technologies, and goes on to note specific dangers, such as criminal use of virtual currencies to hide identity.[88] Much like its FFIEC counterparts, the majority of recent data security regulation from OCC has come in the form of interagency

81. *See* FED. DEPOSIT INS. CORP., *supra* note 77 (establishing general procedures that businesses should follow in regards to data security).

82. *See Supervisory Policy and Guidance Topics*, BD. OF GOVERNORS OF THE FED. RESERVE SYS., https://www.federalreserve.gov/bankinforeg/topics/info_security.htm (last visited Jan. 24, 2017) (listing multiple policy letters relating to customer security).

83. *Id.*

84. INTERAGENCY GUIDELINES ESTABLISHING STANDARDS FOR SAFEGUARDING CUSTOMER INFORMATION, FED. RESERVE SYS. (2001), https://www.federalreserve.gov/boarddocs/srletters/2001/sr0115a1.pdf.

85. *Id.; See Supervisory Policy and Guidance Topics: Information Security*, FED. RESERVE BD., https://www.federalreserve.gov/bankinforeg/topics/info_security.htm (last visited Jan. 24, 2017) (listing the policy letters relating to information security published by the FFIEC)

86. *About the OCC*, OFFICE OF THE COMPTROLLER OF CURRENCY, U.S. DEP'T OF THE TREASURY, https://www.occ.treas.gov/about/what-we-do/mission/index-about.html (last visited Jan. 24, 2017).

87. *See* OFFICE OF THE COMPTROLLER OF CURRENCY, SEMIANNUAL RISK PERSPECTIVE 7 (2016), https://www.occ.gov/publications/publications-by-type/other-publications-reports/semiannual-risk-perspective/semiannual-risk-perspective-spring-2016.pdf (explaining how cyber attacks are one of the primary threats to financial institutions, especially large banks).

88. *Id.* at 7–8.

FFIEC guidance.[89]

In addition to federal regulations, many financial institutions must abide by state-issued rules.[90] In 2016, the state of New York published a proposed rule that, if codified, will make New York the first state to regulate data security at financial institutions.[91] Some of the most noteworthy requirements set forth in the proposal include requiring a written data security program and the designation of a Chief Information Security Officer responsible for overseeing data security programs and policies.[92] These regulations apply to all financial services companies including insurance agencies, with limited exceptions for institutions with fewer than 1000 customers or less than $10 million in year-end assets.[93] Scholars in this field have noted that state-level regulations could act to create an overly complex web of regulations that could, in some instances, be self-conflicting.[94] Allowing such state regulations could distract the financial industry, and cause more harm than good to consumers.[95] To date, there are no other proposed state-level regulations for cybersecurity.[96]

While the aforementioned financial agencies have taken significant steps to regulate data security, the FTC has long served as the primary enforcer in this field.[97] Over the course of the last twenty years the FTC has successfully brought over sixty data security enforcement actions, utilizing jurisdiction that extends to nearly all

89. Cruz & Newman, *supra* note 70.

90. *See Who Regulates My Bank?*, OFFICE OF THE COMPTROLLER OF CURRENCY, https://www.helpwithmybank.gov/national-banks/national-banks.html (last visited Jan. 24, 2017) (establishing that state chartered banks are also regulated by state regulatory bodies).

91. Greg Farrell, *New York Financial Regulator Rolls Out Cybersecurity Proposals*, BLOOMBERG (Sept. 13, 2016, 11:55 AM), https://www.bloomberg.com/news/articles/2016-09-13/new-york-financial-regulator-rolls-out-cybersecurity-proposals.

92. TIFFANY QUACH, PROSKAUER ROSE LLP, NEW YORK DEPARTMENT OF FINANCIAL SERVICES PROPOSES CYBERSECURITY REGULATION (Nov. 7, 2016), http://privacylaw.proskauer.com/2016/11/articles/cybersecurity/new-york-department-of-financial-services-proposes-cybersecurity-regulation/.

93. Kaleigh Simmons, *What New York's Proposed Cybersecurity Regulations Mean for the Rest of the Industry*, RIPPLESHOT (Oct. 5, 2016), http://info.rippleshot.com/blog/what-new-yorks-proposed-cybersecurity-regulations-mean-for-the-rest-of-the-industry.

94. Germano, *supra* note 60.

95. Germano, *supra* note 60.

96. *See* Germano, *supra* note 60 (describing New York as the only state to consider such a rule).

97. Germano, *supra* note 60.

institutions that manage consumer data.[98]

Analyzing the actions of the FTC is particularly useful in this context, as the agency's statutory language governing enforcement is nearly identical to that of the CFPB.[99] More specifically, both agencies have the authority to bring action against parties engaging in unfair, deceptive, or abusive acts or practices ("UDAAP").[100] In *Dwolla*, the prohibition on deceptive acts and practices was at issue, and therefore analyzing the FTC's UDAAP actions can be helpful in understanding the CFPB's enforcement action against Dwolla.[101]

The FTC began policing consumer data security by focusing on its authority to prevent deception,[102] targeting an internet company for its deceptive collection of user information in 1998.[103] Likewise, the majority of the FTC's data security enforcement actions have utilized deception as the primary theory.[104] The FTC's utilization of its UDAAP authority with regards to data security practices has consistently been upheld in federal courts.[105] For example, in *FTC v. Wyndham Worldwide Corp.*,[106] Wyndham challenged an FTC action filed in response to a data breach involving 619,000 customer accounts.[107] The FTC's evidence indicated that Wyndham failed to use firewalls at critical network points, and did not utilize encryption for customer data

98. Woodrow Hartzog and Daniel J. Solove, *The Scope and Potential of FTC Data Protection*, 83 GEO. WASH. L. REV. 2230, 2236 (2016).

99. MARK TAYLOR, PAYMENTS COMPLIANCE, WHAT DOES THE FIRST CFPB ORDER ON DATA SECURITY COMPLIANCE SIGNAL?, 2 (Mar. 16, 2016), http://www.buckleysandler.com/uploads/1082/doc/payments_compliance_-_what_does_the_first_cfpb_order_on_data_security_co___.pdf.

100. FEDERAL RESERVE, FEDERAL TRADE COMMISSION ACT SECTION 5: UNFAIR OR DECEPTIVE ACTS OR PRACTICES 7 (2016), https://www.federalreserve.gov/boarddocs/supmanual/cch/ftca.pdf; Dodd-Frank Wall Street Reform and Consumer Protection Act ("Dodd-Frank") § 1031, 12 U.S.C. § 5531(a) (2015).

101. Dodd-Frank § 1031, 12 U.S.C. § 5531(a); DWOLLA CONSENT ORDER, *supra* note 1, at 4.

102. Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 628 (2014) (analyzing trends from 154 privacy related complaints to form a "common law").

103. *Id.* at 599.

104. Id.

105. *See* FTC v. Wyndham Worldwide Corp., 799 F.3d 236, 242–43 (3d Cir. 2015) (upholding the FTC's data security action against Wyndham Worldwide in the absence of definitive agency guidance); LabMD, Inc., No. 9357, 2015 WL 7575033 *1 (F.T.C. Nov. 13, 2015).

106. *Wyndham*, 799 F.3d 236 (3d Cir. 2015).

107. *Wyndham*, 799 F.3d at 242-43.

files.[108] Wyndham claimed that the FTC's powers over data security were too broad, and that Wyndham had not been given "fair notice" that such an action could be brought against them.[109] Siding with the FTC, the U.S. Court of Appeals for the Third Circuit held that Wyndham did in fact have notice as it could "reasonably foresee" UDAAP actions brought in response to its poor security practices.[110] To determine what Wyndham could "reasonably foresee," the court employed a cost-benefit analysis taken from Wyndham's perspective, where the cost of precautions was weighed against the benefits of preventing a breach.[111]

In *FTC v. LabMD*,[112] the FTC brought action against LabMD for unfairly failing to prevent unauthorized users from accessing patient health information.[113] In this case LabMD challenged the FTC's jurisdiction by asserting that The Health Insurance Portability and Accountability Act of 1996[114] ("HIPAA") was the only data security statute it must comply with.[115] This argument failed as the Administrative Court held that, absent direct statutory language, agency-specific data security laws do not trump the FTC's UDAAP powers.[116] In ruling, the court held that UDAAP powers are intended to be broad, defined predominately in the context of FTC precedent.[117]

In 2007, the FTC issued a guidebook entitled, *Protecting Personal Information: A Guide for Business*.[118] This guidebook recommends that companies: avoid collecting nonessential personal information, restrict employee access to consumer data, test authentication bypass methods, and patch affiliate third-party software.[119] While this guidance is presented as being non-compulsory,

108. *Wyndham*, 799 F.3d at 256.

109. *Id.*; Solove & Hartzog, *supra* note 98, at 2240.

110. *Wyndham*, 799 F.3d at 256.

111. *Id.*

112. LabMD, Inc., No. 9357, 2015 WL 7575033 *1 (F.T.C. Nov. 13, 2015).

113. LabMD, Inc. v. FTC, 776 F.3d 1275, 1277 (11th Cir 2015).

114. Health Insurance Portability and Accountability Act of 1996 ("HIPAA") § 264(a), 42 U.S.C. § 1320(d)(2) (2015).

115. Solove & Hartzog, *supra* note 98, at 2243; Order Denying Respondent LabMD's Motion to Dismiss at *9, LabMD, Inc., No. 9357, 2015 WL 7575033 (F.T.C. Nov. 13, 2015).

116. *Id*. at *11.

117. *Id*. at *12.

118. *See* F.T.C. v. Wyndham Worldwide Corp., 799 F.3d 236, 256 (3d Cir. 2015) (citing FTC guidance published in 2007).

119. *Id.*

the *Wyndham* court considered the guidebook as evidence against Wyndham's "fair notice" argument.[120] While formal FTC guidance could benefit the industry, scholars have noted that a "case-by-case approach" is better suited for dealing with the dynamic issues associated with data security.[121]

The CFPB has consistently relied upon its UDAAP powers as its primary enforcement tool.[122] The popularity of this tool can be attributed partly to the large amount of discretion implicit in this broad statutory language.[123] While deception was the only prong of UDAAP utilized by the CFPB in Dwolla, observers have predicted that, based on FTC precedent, future actions will likely utilize the unfairness prong.[124] Unlike the deceptive prong, Dodd-Frank provides specific explicit definitions for "unfair" and "abusive" practices.[125] Unfairness is found in situations where the act "causes or is likely to cause substantial injury to consumers, and in cases where the injury is not outweighed by countervailing benefits to consumers or to competition."[126] Abusive practices are defined as those that "materially interfere with the ability of a consumer to understand a term or condition of a consumer financial product or service," and therefore take unreasonable advantage of the consumer's expectations and understanding.[127]

While Dodd-Frank does not formally define "deceptive," the agency has published enforcement manuals describing this term as a "representation, omission, act, or practice that is likely to mislead the consumer."[128] The CFPB enforcement manual also holds that evidence of a consumer already being misled is not required, rather the agency must simply prove that the practice is likely to mislead "reasonable

120. *See id.* at 256 (holding that the FTC guidance on cybersecurity did constitute ample fair notice)

121. Solove & Hartzog, *supra* note 98, at 2299.

122. BARLOON ET AL., *supra* note 44.

123. BARLOON ET AL., *supra* note 44.

124. DURBIN & RODRIGUEZ, *supra* note 3.

125. Dodd-Frank Wall Street Reform and Consumer Protection Act ("Dodd-Frank") § 1031, 12 U.S.C. § 5531(c)-(d) (2015).

126. Dodd-Frank § 1031, 12 U.S.C. § 5531(c).

127. Dodd-Frank § 1031, 12 U.S.C. § 5531(d).

128. CONSUMER FIN. PROT. BUREAU, CFPB CONSUMER LAWS AND REGULATIONS: CFPB MANUAL V.2 5 (Oct. 2012), http://www.cfpaguide.com/portalresource/Exam%20Manual%20v%202%20-%20UDAAP.pdf.

consumers."[129] The CFPB utilizes the "four Ps" test to evaluate whether a policy is likely to mislead reasonable consumers.[130] For a written statement, this test focuses on the *prominence* of the statement, how the information is *presented*, the *placement* of the information, and the statement's *proximity* to the claim it qualifies.[131] Furthermore, a subsequent truthful disclosure is not sufficient to cure a deceptive act or promise that occurred in the past.[132] The CFPB's enforcement guide for deceptive acts and practices cites the FTC's Policy Statement on Deception.[133]

In addition to overlapping enforcement statutes, the CFPB and the FTC also have overlapping areas of jurisdiction.[134] The two agencies have multiple Memoranda of Mutual Understanding ("MoUs"), in which they lay out the intricacies of their jurisdictional overlap.[135] Included in their shared powers is the ability to bring enforcement actions against nonbank providers of financial products.[136] These MoUs are intended to prevent duplicative rulemaking and enforcement.[137] These documents also acknowledge that in some circumstances it may be best that the two agencies coordinate their enforcement activities.[138] To prevent duplicative actions, these MoUs require a "notice of commencement of investigation" in which the agencies notify one another of actions that could potentially fall within their overlapping areas of jurisdiction.[139] While these notices are not public record, it is likely that the CFPB notified FTC of its Dwolla investigation, as this company seems to fall under the jurisdiction of both organizations.[140]

---

129. *Id.*

130. *Id.* at 5-6.

131. *Id.*

132. *Id.*

133. *Id.* at 5 n.10.

134. *E.g.*, Memorandum of Understanding Between the Consumer Fin. Prot. Bureau and the Fed. Trade Comm'n (Mar. 6, 2015), https://www.ftc.gov/system/files/documents/cooperation_agreements/150312ftc-cfpb-mou.pdf.

135. *Id.*

136. *Id.*

137. *Id.* at 3.

138. *Id.* at 4.

139. *Id.* at 4.

140. *Id* at 4.

IV. DWOLLA'S IMPACT MOVING FORWARD

Dodd-Frank does not explicitly require the CFPB to regulate data security.[141] The CFPB's expansion into data security, therefore, represents an evolution of the "in connection"[142] language found in Section 1031(a) of Dodd-Frank.[143] In this case, the deceptive data statements were "in connection" with the financial services that Dwolla provided consumers via its payment network.[144]

One of the biggest questions *Dwolla* raises is how the CFPB will work alongside the FTC in enforcing data security.[145] While the two agencies have acknowledged their overlapping powers, neither has gone as far as to claim exclusive jurisdiction over a specific industry.[146] It is difficult to know whether the CFPB will act merely to supplement the data security policies the FTC pursues, or whether the CFPB will implement a different agenda.[147] For now, it is fair for companies subject to overlapping jurisdiction to assume that they may face enforcement actions from either or both agencies.[148]

Companies subject to overlapping jurisdiction should take note of *Dwolla*, as the CFPB examination powers are far superior to those held by the FTC.[149] These powers apply to all "entities and individuals

141. *See* ARNOLD AND PORTER, *supra* note 20, at 1 (describing the areas of the economy over which the CFPB was delegated authority).

142. Dodd-Frank Wall Street Reform and Consumer Protection Act ("Dodd-Frank") § 1031, 12 U.S.C. § 5531 (2015) ("The Bureau may take any action authorized under part E to prevent a covered person or service provider from committing or engaging in an unfair, deceptive, or abusive act or practice under Federal law in connection with any transaction with a consumer for a consumer financial product or service, or the offering of a consumer financial product or service.").

143. Dodd-Frank Wall Street Reform and Consumer Protection Act ("Dodd-Frank") § 1031(a), 12 USC § 5531(a) (2015).; DAVID A. STEIN & CALEB SKEATH, COVINGTON & BURLING LLP, CFPB ACTION SENDS WARNING SIGNAL TO FINANCIAL INSTITUTIONS 9 (2016), https://www.cov.com/-/media/files/corporate/publications/2016/04/cfpb_action_sends_warning_signal_to_financial_institutions.pdf;

144. DWOLLA CONSENT ORDER, *supra* note 1, at *4.

145. Michael Gordon et al., *BNA Insights: The CFPB and Data Security Enforcement*, 106 BANKING REP. (BNA), No. 23 (June 6, 2016), at 4 https://www.wilmerhale.com/uploadedFiles/Shared_Content/Editorial/Publications/Documents/2016-06-15-BNA-INSIGHTS-The-CFPB-and-Data-Security-Enforcement.pdf.

146. CFPB, *supra* note 18, at 5.

147. CFPB, *supra* note 18, at 5.

148. CFPB, *supra* note 18, at 4.

149. *See* CFPB, *supra* note 18 (listing the various investigative tools at the disposal of the CFPB's examiners).

that engage in offering or providing a consumer financial product or service."[150] Companies meeting this description are required to grant CFPB examiners access to a wide range of information including internal policies, audit reports, and training materials.[151] In addition to being able to access these documents, examiners have the right to go on-site to conduct interviews and review documents relevant to their investigations.[152] CFPB examiners may also direct covered entities to adjust their practices through a separate informal process.[153] During this process, the CFPB examiner shares the findings of his or her investigation with the institution, and makes recommendations on how to remedy identified issues.[154] While the CFPB prefers self-correction of these issues, some circumstances require enforcement actions.[155] In this regard, the CFPB's powers are broader than those of the FTC, which is generally limited to issuing civil investigative demands.[156] In addition to broader examination powers, the CFPB can also assess monetary penalties for any UDAAP violation, unlike the FTC, which can only issue fines in a limited set of circumstances.[157]

The CFPB's decision to exercise its powers against Dwolla also introduces a host of questions.[158] The CFPB covers thousands of companies, some of which likely have similar deceptive data security statements in place.[159] The choice of Dwolla as the first target of its kind could be motivated by a desire to put companies in the quickly growing fintech industry on notice.[160] The lack of breach or attempted

150. Dodd-Frank Wall Street Reform and Consumer Protection Act ("Dodd-Frank") § 1024, 12 USC § 5514 (2015).

151. CFPB, *supra* note 18, at 4.

152. CFPB, *supra* note 18, at 5.

153. Gordon et. al., *supra* note 145.

154. CFPB, *supra* note 18.

155. CFPB, *supra* note 18.

156. Gordon et al., *supra* note 145, at 3.

157. Gordon et al., *supra* note 145, at 3.

158. *See* John Stewart, *In Its First Action on Data Security, the CFPB Hits Dwolla With a $100,000 Penalty* (March 3, 2016), http://www.digitaltransactions.net/news/story/In-Its-First-Action-on-Data-Security_-the-CFPB-Hits-Dwolla-With-a-_100_000-Penalty (claiming that this action should put digital money transferring services on notice).

159. *See* Dodd-Frank Wall Street Reform and Consumer Protection Act ("Dodd-Frank") § 1024, 12 USC § 5514 (2015); MORGAN LEWIS, WHITE PAPER: THE CONSUMER FINANCIAL PROTECTION BUREAU: WHAT IT IS AND WHAT TO EXPECT (2012), https://www.morganlewis.com/pubs/lit_whitepaper_consumerfinancialprotectionbureau_jan2012.pdf.

160. John Stewart, *supra* note 158.

breach in *Dwolla* could alternatively signal that the CFPB is focusing more broadly on ensuring covered entities have comprehensive policies, even in the absence of specific security threats.[161] There have been recent FTC complaints filed against Credit Karma and Fandango where deceptive data security practices were also prosecuted without breach.[162] The facts of these cases are similar in that the FTC asserted that these companies had put customers at risk by misrepresenting their security policies and failing to take the steps needed to secure their customer's information.[163]

The CFPB's choice to enforce data security prior to releasing guidance is also potentially strategic.[164] As previously mentioned, the court in *Wyndham* placed significant value in informal guidance documents published by the FTC.[165] However, creating CFPB-specific guidance could be problematic, as it would likely conflict with the data security policies already listed in other examples of agency-specific guidance.[166] Scholars have noted that formal guidance is not well-suited to address the highly dynamic nature of data security issues.[167] The CFPB may therefore intentionally avoid issuing meaningful guidance, and continue to establish precedent through enforcement actions such as this.[168] The relatively meager nature of the fine issued to Dwolla could signal that this action was intended to serve such an informal guidance role.[169]

161. *See*, *We Are Never Done*, DWOLLA (Mar. 2, 2016), https://www.dwolla.com/updates/we-are-never-done/ (reaffirming that no actual data breach has ever occurred at Dwolla); DURBIN & RODRIGUEZ, *supra* note 3.

162. Press Release, FTC, Fandango, Credit Karma Settle FTC Charges that They Deceived Consumers By Failing to Securely Transmit Sensitive Personal Information (March 2014), https://www.ftc.gov/news-events/press-releases/2014/03/fandango-credit-karma-settle-ftc-charges-they-deceived-consumers.

163. *Id*.

164. *See* FTC v. Wyndham Worldwide Corp., 799 F.3d 236, 256 (3d Cir. 2015) (holding that the party could be held liable despite the lack of formal rules on cybersecurity issued by the FTC); *see also* GORDON, *supra* note 145, at 1 ("Despite this enforcement threat, the bureau has provided virtually no guidance on the specific data security practices it expects companies to follow.").

165. *Wyndham*, 799 F.3d at 256.

166. *Id*.

167. Solove & Hartzog, *supra* note 98, at 2299.

168. *See id.* (establishing that previous actions put FTC covered persons on notice).

169. *See* CONSUMER FIN. PROT. BUREAU, *Enforcement Actions*, http://www.consumerfinance.gov/policy-compliance/enforcement/actions/?form-id=0&filter0_title=&filter0_categories=admin-filing&filter0_from_date=&filter0_to_date=. (establishing that fines levied by the CFPB in other cases have been much much larger).

The preventative approach to data security endorsed by the CFPB in *Dwolla* may very well be the most cost-effective, long-term solution for financial institutions.[170] Studies have reinforced the notion that proactive measures reduce overall costs.[171] For example, having a data security team in place can reduce the average cost of breach by 10%, as the company saves significant funds on costly post-breach, third-party remediation.[172] The employee training and planning techniques endorsed in *Dwolla* have also been proven to reduce breach costs.[173]

Companies covered by the CFPB could also benefit from following the National Institute of Standards and Technologies ("NIST") framework.[174] NIST is an organization housed within the Department of Commerce, which works to provide American industry with tools and guides that facilitate both efficiency and productivity.[175] The FTC has acknowledged NIST's framework as consistent with both its guidance and its enforcement actions.[176] At its core, the framework has five functions: identify, protect, detect, respond, and recover.[177] While these steps are broad, they encompass the notion that companies need to be both proactive and reactive in their efforts to protect data.[178] "Identify" includes using data to determine where and how different security threats will develop.[179] "Protect" includes taking proactive steps such as increasing employee awareness, and developing security safeguards in delivery of services.[180] "Detect" concerns the identification of attacks, and the FTC has brought many actions based

170. *See* PONEMON INST., 2016 COST OF DATA BREACH STUDY 9 (June 2016) (establishing that data loss prevention technologies reduce the cost of a data breach), https://public.dhe.ibm.com/common/ssi/ecm/se/en/sel03094usen/SEL03094USEN.PDF.

171. IBM, *supra* note 6 at 9.

172. IBM, *supra* note 6, at 9.

173. IBM, *supra* note 6, at 9. (concluding that employee training reduces the overall costs of a breach by 7% per capita and having BCM measures in place reduces the costs by about 6% per capita).

174. Andrea Arias, *The NIST Cybersecurity Framework and the FTC*, F.T.C. BUS. BLOG (Aug. 31, 2016, 6:36 PM), https://www.ftc.gov/news-events/blogs/business-blog/2016/08/nist-cybersecurity-framework-ftc.

175. *About NIST*, NIST, https://www.nist.gov/about-nist (last visited Jan. 24, 2017).

176. Arias, *supra* note 174.

177. Arias, *supra* note 174.

178. Arias, *supra* note 174.

179. Arias, *supra* note 174.

180. Arias, *supra* note 174.

on companies' failure in this area.[181] Finally, "respond" and "recover" both address the steps companies should have in place to mitigate damage after a breach has occurred.[182] Past FTC actions have stressed the importance of consumer interests in recovery, which can include promptly notifying customers about what information has been compromised.[183] Somewhat ironically, the CFPB's internal data security programs have been analyzed and held to NIST standards by the Office of Inspector General for the Board of Governors of the Federal Reserve System.[184]

Companies can also reduce their potential exposure by simply not collecting personal information.[185] While the nature of the financial industry often necessitates the collection of such information, companies could limit the amount of personal information by adopting technologies such as OAuth.[186] This technology provides temporary access to personal information stored by social networking companies, (e.g., Facebook profile information) thereby limiting the quantity of information needed for customer registration.[187]

To avoid deception violations, financial institutions must be careful when drafting privacy policies and other documents that will be distributed to customers.[188] As long as the CFPB is acting on the deception prong alone, companies can protect themselves by avoiding misleading security statements.[189] This could be as easy as telling consumers in disclaimers that "we cannot guarantee absolutely that your

181. Arias, *supra* note 174.

182. Arias, *supra* note 174.

183. Arias, *supra* note 174.

184. BD. OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM & CONSUMER FIN. PROT. BUREAU, 2015 AUDIT OF THE CFPB'S INFORMATION SECURITY PROGRAM 11 (Nov. 2015), https://oig.federalreserve.gov/reports/cfpb-2015-information-security-program-nov2015.pdf.

185. *See* Joel Schectman, *5 Reasons Too Much Data Can be Risky*, WALL ST. J. (Apr. 10, 2014, 6:31 PM) http://blogs.wsj.com/briefly/2014/04/10/5-reasons-too-much-data-can-be-risky/ (establishing that unnecessary data collection posses a variety of dangers including increased exposure to hackers and possible damage to public perception when the scope of data collection is revealed).

186. OAuth is a security protocol that allows users to login and provide access to information that they provided another online service provider (e.g., "Login with Facebook"). Changhun Oh, *Dancing with OAuth: Understanding how Authorization Works*, CUBRID (2012), http://www.cubrid.org/blog/dev-platform/dancing-with-oauth-understanding-how-authorization-works/.

187. *Id.*

188. TAYLOR, *supra* note 99, at 1.

189. TAYLOR, *supra* note 99.

information will never be subject to a breach."[190] If companies prefer to make a guarantee about data security, they should avoid grandiose statements such as those made by Dwolla, as these are far more likely to be flagged for possible deception.[191] This implicates a balancing act where companies must craft statements that give their customers sufficient confidence, while not creating liability.[192] Attorneys in the field have noted that to be taken seriously, companies must at least portray that their policies meet industry standards.[193]

Shortly after the CFPB's enforcement action, Dwolla published a blog post about its data security policies entitled "We Are Never Done."[194] In the post, Dwolla concedes that "we may not have chosen the best language and comparisons to describe some of our capabilities," and that "it has never been the company's intent to mislead anyone on critical issues like data security."[195] Dwolla also emphasized that its customers' accounts have never been breached.[196] The post concludes with a brief description of the encryption methods utilized by Dwolla, including a promise that Dwolla will never stop pursuing security for customers.[197]

V. CONCLUSION

Agency focus on data security is likely to grow as the threat and scope of cyber attacks increase.[198] The CFPB is not the first to police data security, but the agency's strong enforcement tools and focus on consumer protection make it a formidable regulator.[199] While the *Dwolla* consent order provides some useful guidance, uncertainty remains the prevailing theme. The decision to bring action against

190. TAYLOR, *supra* note 99.

191. TAYLOR, *supra* note 99.

192. *See* TAYLOR, *supra* note 99 (asserting that in light of the Dwolla consent order companies must be extremely careful when determining the scope of their privacy statements).

193. TAYLOR, *supra* note 99, at 1.

194. Dwolla, *supra* note 161.

195. Dwolla, *supra* note 161.

196. Dwolla, *supra* note 161.

197. Dwolla, *supra* note 161; At the time of this writing, Dwolla's website included the less aggressive claim that it is working with "top security industry professionals to build and maintain the platform, and keep customer information secure." Dwolla, *supra* note 161.

198. TAYLOR, *supra* note 99.

199. DURBIN & RODRIGUEZ, *supra* note 3.

Dwolla may have been strategic, but without further enforcement actions it is impossible to discern the CFPB's regulatory priorities in this field.[200] The election of President Donald J. Trump has created further uncertainty, as his administration has expressed plans to make broad changes to the CFPB's personnel.[201] Until clarification is provided in the form of further enforcement actions or guidance, financial institutions should utilize both FTC precedent and the *Dwolla* consent order to assess the adequacy of their data security policies.[202]

GRAHAM T. DEAN*

200. TAYLOR, *supra* note 99.

201. Yuka Hayashi, *Trump Administration Looks to Restructure CFPB*, WALL ST. J. (Feb. 3, 2017), https://www.wsj.com/articles/trump-administration-looks-to-restructure-cfpb-1486116000.

202. *Id; See* TAYLOR, *supra* note 99 (describing the similarities between the FTC and CFPB in enforcing data security).

* I would like to thank Vinita Tandon, Ariana Johnson, and all the other editors that assisted me during the drafting process. Further, I would like to thank my father, Larry Dean, for his unwavering support.